UNITED STATES BANKRUPTCY COURT
EASTERN DISTRICT OF MISSOURI
ST. LOUIS DIVISION

IN RE:	Chapter 11
	Case No. 25-40976
23ANDME HOLDING CO., et al.,[1]	
	Joint Administration Requested
Debtors.	

NOTICE BY THE STATE OF INDIANA REGARDING THE DEBTORS' OUTSTANDING REGULATORY SECURITY AND PRIVACY ISSUES

COMES NOW, the State of Indiana ("State"), by and through Counsel, and files this *Notice Regarding the Debtors' Outstanding Regulatory Security and Privacy Issues*, and states as follows:

I. OVERVIEW

The Debtors' business is built upon the DNA of millions of consumers in America and throughout the world. The Debtors collect consumers' physical DNA samples ("Genetic Material") and analyze the Genetic Material to derive data ("Genetic Data") and create reports on consumers' ancestry, genetic characteristics, and probable genetic health risks. After the Debtors analyze Genetic Material, it may be stored by the Debtors or the Debtors' "biobank."[2] In addition to Genetic Material and Genetic Data, the Debtors collect and maintain consumers' self-reported health

[1] A complete list of each of the Debtors in these chapter 11 cases may be obtained on the website of the Debtors' proposed claims and noticing agent at https://restructuring.ra.kroll.com/23andMe. The Debtors' service address for purposes of these chapter 11 cases is: 870 Market Street, Room 415, San Francisco, CA 94102.

[2] *Biobanking Consent Document*, available at: https://www.23andme.com/about/biobanking/ (last visited Mar. 24, 2025) ("This biobanking consent applies to any biological specimens (including saliva, blood, microbiome, tissue samples, etc.) you provide to 23andMe in order to receive a 23andMe Service and/or as part of a 23andMe Research study.").

information, including disease conditions, family history, and other traits ("Self-Reported Health Information").[3] The Genetic Material, Genetic Data, and Self-Reported Health Information the Debtors collect and maintain may be used in medical research conducted by the Debtors or third parties.[4] Finally, the Debtors offer consumers online telehealth visits through their Lemonaid Health subsidiary, offer consumers prescriptions by mail through their Lemonaid Pharmacy subsidiary, and collect and store medical records for these consumers ("Medical Data").[5]

Since late 2023, the State has been investigating the Debtors due to a serious data breach publicly announced by 23andMe in October 2023, which impacted the sensitive data of at least 6.9 million consumers nationwide.[6] Based upon this ongoing

---

[3] *23andMe Privacy Statement*, available at: https://www.23andme.com/legal/privacy/full-version/ (last updated Sep. 24, 2024) (last visited Mar. 24, 2025).

[4] *Research Consent Document*, available at: https://www.23andme.com/about/consent/ (last visited Mar. 24, 2025) ("The purpose of 23andMe Research is to make new discoveries about genetics and other factors behind diseases and traits. . . . Some 23andMe Research is conducted in collaboration with third parties, such as non-profit organizations, pharmaceutical companies, or academic institutions. . . .).

[5] *Lemonaid Consent to Telehealth*, available at: https://www.lemonaidhealth.com/legals/consent-to-telehealth (last visited Mar. 24, 2025) ("Lemonaid Health is an online doctor's office. . . . Our medical team is made up of doctors and nurse practitioners. . . . We are an online doctor's office and not a pharmacy. If you request that your medicines be delivered to you in the mail, we'll arrange for Lemonaid Pharmacy LLC or an independent pharmacy to mail your medicines."); *Lemonaid Privacy Policy*, available at: https://www.lemonaidhealth.com/legals/privacy-policy (last updated Mar. 14, 2025) (last visited Mar. 24, 2025) (identifying "Information We Collect" as including "Health Information: information you provide to us or our Medical Team, including information we generate about you, related to your physical, mental or other health conditions."); *see also 23andMe Medical Record Privacy Notice*, available at: https://www.23andme.com/legal/medical-record-privacy-notice/ (effective Sep. 24, 2024) (last visited Mar. 24, 2025) ("customers have an opportunity to participate in Telehealth Services coordinated through 23andMe and its service providers, subsidiaries, and affiliates, including Lemonaid Health, Inc. . . . This notice covers how your Medical Record Information is used, disclosed, and maintained").

[6] *Addressing Data Security Concerns – Action Plan*, available at: https://blog.23andme.com/articles/addressing-data-security-concerns (last updated Dec. 5, 2023) (last visited Mar. 24, 2025).

investigation, the State has found serious issues with 23andMe's data security procedures, and the State has been working with the Debtors to reach agreed terms to address these issues, but to date, no resolution has been reached.[7]

Due to the highly sensitive nature of the Debtors' business, and the speed at which bankruptcy cases progress, the State files this Statement out of an abundance of caution and to put all parties on notice of the regulatory issues that will need to be addressed in any sale or transfer of the Debtors' business or assets.

II. THE DEBTORS HOLD MILLIONS OF CONSUMERS' HIGHLY SENSITIVE PHYSICAL GENETIC MATERIAL, GENETIC DATA, SELF-REPORTED HEALTH INFORMATION, MEDICAL DATA, AND OTHER DATA

The Debtors' business model relies on the collection and storage of highly sensitive Genetic Material, Genetic Data, Self-Reported Health Information, and Medical Data, along with other types of sensitive consumer data. The Debtors collect a wide range of data types during their regular course of business, and the Debtors have amassed a trove of sensitive data on millions of Americans.[8] 23andMe discloses collecting the following types of personal information from consumers:

- **Registration Information:** information you provide during account registration or when purchasing the Services, such as a name, user ID, password, date of birth, billing address, shipping address, payment information (e.g., credit card), account authentication information, or contact information (e.g., email, phone number).

[7] At this time, the State has not filed a lawsuit against the Debtor; however, the State reserves the right to bring any police and regulatory action necessary to protect the health and safety of its citizens.

[8] *See, e.g.*, *23andMe Reports FY2023 Fourth Quarter and Full Year Financial Results* (May 25, 2023), https://investors.23andme.com/news-releases/news-release-details/23andme-reports-fy2023-fourth-quarter-and-full-year-financial ("We grew our customer base to over 14 million genotyped customers").

- **Genetic Information:** information regarding your genotype (e.g., the As, Ts, Cs, and Gs at particular locations in your DNA). Genetic Information includes the 23andMe genetic data and reports provided to you as part of our Services.

- **Sample Information:** information regarding any sample, such as a saliva sample, that you submit for processing to be analyzed to provide you with Genetic Information, laboratory values or other data provided through our Services.

- **Self-Reported Information:** information you provide to 23andMe including your gender, disease conditions, health-related information, traits, ethnicity, family history, or anything else you provide to us within our Service(s).

- **Biometric information:** certain Self-Reported Information you provide to us or our service providers to verify your identity using biological characteristics.

- **User Content:** information, data, text, software, music, audio, photographs, graphics, video, messages, or other materials, other than Genetic Information and Self-Reported Information, generated by users of 23andMe Services and transmitted, whether publicly or privately, to or through 23andMe. For example, User Content includes comments posted on our Blog or messages you send through our Services.

- **Web-Behavior Information:** information on how you use our Services or about the way your devices use our Services is collected through log files, cookies, web beacons, and similar technologies (e.g., device information, device identifiers, IP address, browser type, location, domains, page views).[9]

Likewise, Lemonaid Health discloses collecting the following types of personal information from consumers:

- "Individual health conditions, treatment, diseases, or diagnosis; Social, psychological, behavioral, and medical interventions; Use or purchase of prescribed medication; Diagnoses or diagnostic testing,

[9] *23andMe Privacy Statement*, available at: https://www.23andme.com/legal/privacy/full-version/ (last updated Sep. 24, 2024) (last visited Mar. 24, 2025).

treatment, or medication; Reproductive or sexual health information"

- "Biometric data"
- "Genetic data"
- "[P]hotos you provide to us to verify your identity before beginning a virtual visit"
- "[A]ge (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, and genetic information (including familial genetic information)"
- "[D]ata that reveals your: social security, driver's license, state identification card, or passport number; account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to your account; precise geolocation"[10]

III. DEBTORS PROMISED THAT CONSUMERS' SENSITIVE DATA WOULD BE PROTECTED AND CONSUMERS CAN CONTROL HOW THEIR DATA IS USED

The Debtors have repeatedly promised consumers that their sensitive data is protected and that consumers control whether and how their data is used. 23andMe's Privacy Statement assures customers "It's your data" and explains that customers have the right to delete their account "at any time."[11] Further, "Upon account deletion, we will automatically opt you out of Research and discard your sample."[12]

[10] *Lemonaid Privacy Policy*, available at: https://www.lemonaidhealth.com/legals/privacy-policy (last updated Mar. 14, 2025) (last visited Mar. 24, 2025).
[11] *23andMe Privacy Statement*, available at: https://www.23andme.com/legal/privacy/full-version/ (last updated Sep. 24, 2024) (last visited Mar. 24, 2025).
[12] *Id.*

However, even if a customer does not wish to delete his or her account, the Privacy Statement provides that a customer's data will not be used for research purposes without the customer's prior consent. The Privacy Statement provides:

> [T]aking part in 23andMe Research is completely voluntary. . . . If you are eligible to participate in Research, you choose whether to participate or not, and you can change your mind any time. Customers never need to participate in Research to use 23andMe. . . . We do not use your information for Research unless you explicitly choose to participate in Research.

23andMe's Research Consent Document makes similar representations:

> **23andMe uses physical, technical, and administrative security measures to protect your information.** We regularly review and improve our privacy and security practices to help ensure the safety of your information. . . . Your participation in the 23andMe Research study is **completely voluntary**, so you may choose to not participate. If you change your mind about participating, you can **change your consent choice** in your Account Settings at any time. If you withdraw your consent, 23andMe will prevent your Research Information from being used in new 23andMe Research initiated after 30 days from when we receive your request from your Account Settings.[13]

Likewise, even if a customer does not wish to delete his or her account, 23andMe's Privacy Statement provides that a customer can opt-out of sample storage and choose to discard his or her Genetic Material sample.[14] 23andMe's Biobanking Consent Document similarly provides:

> **Participation Is Voluntary**
>
> Taking part in our biobank is voluntary and entirely your choice. If you do not consent to have your Samples stored, it will not impact your ability to receive or participate in the 23andMe Service for which you

[13] *Research Consent Document*, available at: https://www.23andme.com/about/consent/ (last visited Mar. 24, 2025) (Emphasis in original).
[14] *23andMe Privacy Statement*, available at: https://www.23andme.com/legal/privacy/full-version/ (last updated Sep. 24, 2024) (last visited Mar. 24, 2025).

> submitted your Samples, and your Samples will be securely discarded after completion of the analysis for which it was submitted.
>
> **Privacy**
>
> All of the same protections, terms, and safeguards described in our Terms of Service and Privacy Statement will apply to the storage of your Samples and any information generated from our further analysis of your Samples. . . . 23andMe uses a range of physical, technical, and administrative procedures to protect the security and privacy of your Personal Information, including your Samples and the data generated from the analysis of your Samples.
>
> **Withdrawing Your Consent**
>
> You may withdraw your consent to biobanking at any time via your account settings. . . . Once you withdraw your biobanking consent, 23andMe will securely discard your stored Samples within the legally applicable timeframe. Please note that if you delete your 23andMe account, your stored Samples will be securely destroyed.[15]

Significantly, 23andMe's Privacy Statement also tells customers that if the company is involved in a bankruptcy, reorganization, or asset sale, the Privacy Statement will apply to their personal information transferred to a new entity through such bankruptcy, reorganization, or asset sale.[16]

[15] *Biobanking Consent Document*, available at: https://www.23andme.com/about/biobanking/ (last visited Mar. 24, 2025).

[16] *23andMe Privacy Statement*, available at: https://www.23andme.com/legal/privacy/full-version/ (last updated Sep. 24, 2024) (last visited Mar. 24, 2025) ("If we are involved in a bankruptcy, merger, acquisition, reorganization, or sale of assets, your Personal Information may be accessed, sold or transferred as part of that transaction and this Privacy Statement will apply to your Personal Information as transferred to the new entity.").

Finally, the current Lemonaid Privacy Policy states: "It's your data, you're in control. . . . You can delete your Lemonaid account and data at any time by contacting us at privacy@lemonaid.com."[17]

III. THE DATA BREACH AND THE STATE'S INVESTIGATION

On October 6, 2023, 23andMe released a blog post disclosing that customer data had been compiled and exfiltrated without authorization by a threat actor using compromised 23andMe user accounts.[18] Through this "Credential Stuffing Incident" the threat actor was able to access roughly 14,000 user accounts and then use the compromised accounts to access "DNA Relatives" and "Family Tree" profiles connected to the compromised accounts, resulting in the compromise of at least 6.9 million profiles, nearly half of the company's customer base.[19] 23andMe later admitted that the data breach started months earlier, in April of 2023, and that 23andMe failed to detect the incident for approximately five months.[20] Although 23andMe failed to require use of multi-factor authentication to secure customer accounts until *after* the data breach,[21] and widely used security standards

[17] *Lemonaid Privacy Policy*, available at: https://www.lemonaidhealth.com/legals/privacy-policy (last updated Mar. 14, 2025) (last visited Mar. 24, 2025).
[18] *Addressing Data Security Concerns – Action Plan*, 23ANDME BLOG (last updated Dec. 5, 2023), https://blog.23andme.com/articles/addressing-data-security-concerns.
[19] *Id.* ("The threat actor used the compromised credential stuffed accounts to access the information included in a significant number of DNA Relatives profiles (approximately 5.5 million) and Family Tree feature profiles (approximately 1.4 million)").
[20] *23andMe admits it didn't detect cyberattack for months*, TECH CRUNCH (Jan. 25, 2024), https://techcrunch.com/2024/01/25/23andme-admits-it-didnt-detect-cyberattacks-for-months/.
[21] *Enhanced Customer Security at 23andMe with 2-Step Verification*, 23ANDME BLOG (Nov. 6, 2023), https://blog.23andme.com/articles/enhanced-customer-security-at-23andme-with-2-step-verification ("Since 2019, 23andMe customers have had the option to utilize authenticator app 2-factor authentication, which adds an extra layer of security to their

recommend screening user passwords for known breached passwords,[22] 23andMe blamed its customers for the data breach, specifically for "negligently recycl[ing] and fail[ing] to update their passwords following . . . past security incidents[.]"[23] After the breach, sensitive data stolen from 23andMe customers was posted on the dark web for sale, including targeted sales of the data of at least 1 million individuals with Ashkenazi Jewish heritage, as well as hundreds of thousands of individuals with Chinese ancestry.[24] This targeting raised significant privacy and personal safety concerns and demonstrates a real risk of harm to consumers when such data is not properly safeguarded. Similarly, in separate incident prior to the 2023 breach, a 23andMe API[25] was used to "block people from sites and apps based on their gender,

---

account. Starting today, we are requiring all customers use a second step of verification to sign into their account.").

[22] *See, e.g.*, *Pwned Passwords*, HAVE I BEEN PWNED? https://haveibeenpwned.com/Passwords (last visited Mar. 24, 2025) (providing a service to determine if a password has been exposed in a prior data breach, explaining "The Pwned Passwords service was created in August 2017 after NIST released guidance specifically recommending that user-provided passwords be checked against existing data breaches."); NIST Special Publication 800-63B, *available at*: https://pages.nist.gov/800-63-3/sp800-63b.html ("Users' password choices are very predictable, so attackers are likely to guess passwords that have been successful in the past. These include dictionary words and passwords from previous breaches, such as the "Password1!" example above. For this reason, it is recommended that passwords chosen by users be compared against a 'black list' of unacceptable passwords. This list should include passwords from previous breach corpuses . . . .").

[23] *23andMe tells victims it's their fault that their data was breached*, TECH CRUNCH (Jan. 3, 2024), https://techcrunch.com/2024/01/03/23andme-tells-victims-its-their-fault-that-their-data-was-breached/.

[24] *23andMe User Data Stolen in Targeted Attack on Ashkenazi Jews,* WIRED (Oct. 6, 2023) https://www.wired.com/story/23andme-credential-stuffing-data-stolen/ ("Hackers posted an initial data sample on the platform BreachForums earlier this week, claiming that it contained 1 million data points exclusively about Ashkenazi Jews. There also seem to be hundreds of thousands of users of Chinese descent impacted by the leak.").

[25] "An API, or application programming interface, is a set of rules or protocols that enables software applications to communicate with each other to exchange data, features and functionality." *What is an API?*, IBM (Apr. 9, 2024), https://www.ibm.com/think/topics/api.

ancestry and any genetic characteristic," in what one reporter called "a race wall around the web".[26] In short, the data is highly sensitive, and past events demonstrate significant potential for misuse.

Since late 2023, the State has been investigating the Debtors, particularly 23andMe, pursuant to state consumer protection laws. Through civil investigative demands, the State has obtained documents and information, and based upon this ongoing investigation, the State has found serious issues with 23andMe's data security procedures. The State has been working with the Debtors to reach agreed terms to address these issues, but to date, no resolution has been reached. At this time, the State has not filed a lawsuit against the Debtors; however, the State reserves the right to bring any police and regulatory action necessary to protect the health and safety of its citizens.

IV. REGULATORY AND SECURITY CONCERNS TO BE ADDRESSED IN ANY SALE OR TRANSFER OF CONSUMER DATA

As the Debtors collect and maintain a large number and variety of sensitive data types, the State would need to be assured that there are sufficient Information Security and Privacy Programs in place with any purchaser of any or all of the information held by the Debtors. The State has regulatory powers and duties to ensure that the personal information of its citizens is secured and safeguarded, and that its citizens, as consumers, are treated fairly. As such, the State would advocate

[26] *How one coder used 23andMe to create a race wall around the web*, WIRED (Jul. 23, 2015), https://www.wired.com/story/23andme-api-blocks-based-on-race-gender/ (noting the code's creator, who was not affiliated with 23andMe, explained online that "Hasidic jews might like to bar access for Ashkenazi or Sephardic jews, or the NAACP might want to filter its prospective members").

that any purchaser be prepared to implement appropriate processes and procedures to comply with regulatory requirements, including for the State of Indiana, the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 *et seq*. Those processes and procedures would likely include: (1) implementing or complying with an Information Security Program that takes into account the size and complexity of the operations and activities of the company and the sensitivity of the stored information; (2) implementing or complying with a Privacy Program for the privacy of consumers including reasonable safeguards and consent and disclosure requirements; (3) requirements related to future incident and breach response and notification; (4) specific technical safeguards and controls such as requiring multi-factor authentication or equivalent enhanced authentication measures; and (5) maintaining customers' ability to require that their physical Genetic Material be destroyed and their data be deleted.

** REMAINDER OF PAGE INTENTIONALLY LEFT BLANK **

V. CONCLUSION

The States ask this Court, Debtors, and any potential purchasers to ensure that any sale of any personal information include terms of protection and notifications to consumers of the protections they can expect. The State of Indiana reserves the right to seek the appointment of a consumer privacy ombudsman in this case.

Respectfully submitted,

By: /s/ Heather M. Crockett
Heather M. Crockett
Deputy Attorney General
Indiana Office of Attorney General
IGCS-5th Floor
302 West Washington Street
Indianapolis, IN 46204-2770
Telephone: 317-233-6254
Facsimile: 317-232-7979
Email: Heather.Crockett@atg.in.gov

CERTIFICATE OF SERVICE

I certify that a true and correct copy of the foregoing has been served via the Court's Electronic Filing System on all parties requesting notice in this proceeding on March 26, 2025.

/s/ Heather M. Crockett
Heather M. Crockett